

CLAIMS

1. A method of recording and/or reproducing data to a recording medium, comprising steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for recording or reproduction of the main data to or from the recording medium; and

recording or reproducing the main data to or from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

2. The method according to claim 1, wherein:

the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and

data are recorded to or reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

3. The method according to claim 1, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with

the user identification data read from the data recorder/player being taken as an encryption key and then recorded to the recording medium.

4. The method according to claim 3, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium.

5. The method according to claim 3, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium.

6. The method according to claim 1, wherein:

the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and

main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

7. The method according to claim 6, further comprising a step of permitting the data reproduction from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a specific identification data.

8. The method according to claim 7, wherein the specific identification data indicates that the recording medium is an original one.

9. The method according to claim 1, wherein the user identification data read from the data recorder/player is set by the user.
10. The method according to claim 9, wherein the user identification data is a data including a user name.
11. A method of recording data to a recording medium, comprising steps of:
comparing a user identification data read from a recording medium having recorded the user identification data along with main data, with a one read from a data recorder/player, for recording the main data to the recording medium; and
recording the main data to the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.
12. The method according to claim 11, wherein:
the recording medium has further recorded therein a management data to manage recording to the recording medium; and
main data are recorded to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.
13. The method according to claim 11, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an

encryption key and then recorded to the recording medium.

14. The method according to claim 13, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium.

15. The method according to claim 14, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium.

16. The method according to claim 11, wherein the user identification data read from the data recorder/player is set by the user.

17. The method according to claim 16, wherein the user identification data includes a user name.

18. A recording-medium recorder comprising:

- a head to scan a recording medium having stored therein a user identification data along with main data;

- a memory having a user identification data recorded therein; and

- a controller to compare the user identification data read by the head from the recording medium with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

19. The apparatus according to claim 18, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller controls the head to record main data to the recording medium.

20. The apparatus according to claim 18, wherein the memory is provided in a user identification data server connected to the data recorder/player.

21. The apparatus according to claim 20, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.

22. The apparatus according to claim 21, wherein when the authentication has successfully be made made, the controller instructs the user identification data server to read the user identification data from the memory.

23. The apparatus according to claim 22, wherein the user identification data read from the memory is encrypted and sent from the user identification data server to the controller.

24. The apparatus according to claim 21, wherein when the authentication has not successfully be made, the controller ceases the operations of recording to the recording medium.

25. The apparatus according to claim 21, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.

26. The apparatus according to claim 19, wherein:

the recording medium has further recorded therein a management data to manage recording to the recording medium; and

the controller records main data to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the memory.

27. The apparatus according to claim 26, where when the user identification data read from the recording medium is coincident with that read from the memory, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded by the head to the recording medium.

28. The apparatus according to claim 27, wherein the user identification data read from the memory is buried in main data to be recorded to the recording medium.

29. The method according to claim 28, wherein the controller encrypts the user identification data read from the memory and buries it in main data to be recorded to the recording medium.

30. The apparatus according to claim 18, wherein a user identification data set by the user is written to the memory.

31. The apparatus according to claim 18, wherein the user identification data to be stored into the memory is set by the user.

32. The apparatus according to claim 31, wherein the user identification data includes a user name.

33. A recording-medium playback method, comprising steps of:

comparing a user identification data read from a recording medium having

recorded therein the user identification data along with main data, with a one read from a data recorder/player, for reproducing the main data from the recording medium; and

reproducing the main data from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

34. The method according to claim 33, wherein:

the recording medium has further recorded therein a management data to manage the operations of data reproduction from the recording medium; and

main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

35. The method according to claim 34, wherein when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a specific identification data, playback of the recording medium is allowed.

36. The method according to claim 35, wherein the specific identification data indicates that the recording medium is an original one.

37. The method according to claim 33, wherein:

the recording medium has encrypted data recorded therein; and

main data read from the recording medium are decrypted using, as an

encryption key, the user identification data read from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

38. The method according to claim 33, wherein the user identification data read from the data recorder/player is set by the user.

39. The method according to claim 38, wherein the user identification data includes a user name.

40. A recording-medium player comprising:

a head to scan a recording medium having recorded therein encrypted data as well as at least a user identification data and reproduction management data;

a memory having a user identification data stored therein; and

a controller to compare the user identification data read by the head from the recording medium, with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

41. The apparatus according to claim 40, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller allows to reproduce main data from the recording medium.

42. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller decrypts main data read by the head from the recording medium using the user identification data.

43. The apparatus according to claim 42, wherein when the user identification data read by the head from the recording medium cannot be detected, the controller controls the operations for playback of the recording medium based on the reproduction management data read from the recording medium.
44. The apparatus according to claim 40, wherein the memory is provided in a user identification data server connected to the data recorder/player.
45. The apparatus according to claim 40, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.
46. The apparatus according to claim 45, wherein when the authentication has successfully be made, the controller instructs the user identification data server to read the user identification data from the memory.
47. The apparatus according to claim 46, wherein the user identification data read from the memory is encrypted and sent from the user identification data server.
48. The apparatus according to claim 45, wherein when the authentication has not successfully be made, the controller ceases the operations for data reproduction from the recording medium.
49. The apparatus according to claim 40, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.

50. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is not coincident with that read from the memory and also when the user identification data read from the recording medium is a specific identification data, the controller allows to reproduce data from the recording medium.

51. The apparatus according to claim 50, wherein the specific identification data indicates the recording medium is an original one.

52. The apparatus according to claim 50, wherein the user identification data set by the user is written to the memory.

53. The apparatus according to claim 40, wherein the user identification data read from the recording medium is set by the user.

54. The apparatus according to claim 53, wherein the user identification data includes a user name.

55. A method of controlling data copying, comprising steps of:

comparing a user identification data read from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for copying the main data; and

controlling data output when the user identification data extracted from the data is coincident with that read from the data recorder/player.

56. The method according to claim 55, wherein:

the main data further includes a management data to manage the operations of copying the data; and

the data copying is controlled based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

57. The method according to claim 56, wherein when the user identification data extracted from the main data is coincident with that read from the data recorder/player, the user identification data extracted from the main data is encrypted using the user identification data as an encryption key before being outputted.

58. The method according to claim 57, wherein the user identification data read from the data recorder/player is buried in the main data.

59. The method according to claim 57, wherein the user identification data read from the data recorder/player is encrypted and buried into the main data.

60. The method according to claim 56, wherein when the management data indicates that billing has to be done for copying the main data, it is judged whether the billing is possible, and the copying is done when the result of judgment is that the billing is possible.

61. The method according to claim 60, wherein the billing is such that a number of times main data can be copied is decremented.

62. The method according to claim 61, wherein when it is judged that the billing is not possible and also when the number of times main data can be copied is not incremented, the copying operation is ceased.

63. The method according to claim 55, wherein the user identification data read

from the data recorder/player is set by the user.

64. The method according to claim 63, wherein the user identification data includes a user name.

65. A data reproducing method comprising steps of:

comparing a user identification data extracted from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for reproduction of the main data; and

reproducing the main data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

66. The method according to claim 65, wherein:

the main data further includes a management data to manage the operation of reproducing the main data; and

the main data are reproduced based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

67. The method according to claim 66, wherein when the user identification data cannot be detected from the main data, the operation of reproducing the main data is controlled based on the management data.

68. The method according to claim 66, wherein when the user identification data extracted from the main data is not coincident with that read from the data recorder/player and also when the user identification data extracted from the main data

is a specific identification data, it is allowed to reproduce the main data.

69. The method according to claim 68, wherein the specific identification data indicates that the recording medium is an original one.

70. The method according to claim 66, wherein when the management data indicates that billing has to be done for reproduction of the main data, it is judged whether the billing is possible, and the main data are reproduced when the result of judgment is that the billing is possible.

71. The method according to claim 70, wherein the billing is made by decrementing a number of times the reproduction can be done.

72. The method according to claim 71, wherein when it is judged that the billing is not possible and also when the number of times of reproduction is not incremented, the operation of reproduction is inhibited.

73. The method according to claim 65, wherein:

the main data includes encrypted data; and

the user identification data extracted from the main data is decrypted using the user identification data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

74. The method according to claim 65, wherein the user identification data read from the data recorder/player is set by the user.

75. The method according to claim 74, wherein the user identification data includes a user name.